PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Jonathan GOLDSTONE

Docket No: Q63477

Appln. No.: 10/058,189

Group Art Unit: 2625

Confirmation No.: 3944

Examiner: Joseph R. POKRZYWA

Filed: January 29, 2002

For: ENCRYPTED E-MAIL MESSAGE RETRIEVAL SYSTEM

DECLARATION UNDER 37 C.F.R. § 1.131

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

I, Jonathan Goldstone, hereby declare and state as follows:

1. I am the inventor named in the above-captioned U.S. Application No. 10/058,189, filed January 29, 2002.

2. At the time I invented the present invention, I was employed by COMVERSE NETWORK SYSTEMS, LTD. (hereinafter "Comverse").

3. Prior to October 25, 2001, the filing date of U.S. Provisional Application No. 60/330,608, the invention as described and claimed in the above referenced application was completed at Comverse, as evidenced by the following:

4. Prior to October 25, 2001, having earlier conceived the idea as set forth in the specification of the above referenced application, I prepared three invention disclosures describing the present invention, and submitted the invention disclosures to Hananel Kvatinsky, Director of Intellectual Property for Comverse, for the purpose of obtaining approval for filing a

patent application in the United States. On March 5, 2001, Mr. Kvatinsky sent a request to Mr. William Mandir of SUGHRUE MION, PLLC of Washington, D.C. requesting the preparation and filing of a patent application with the U.S. Patent and Trademark Office. A copy of the email from Mr. Kvatinsky to Mr. Mandir is provided in Exhibit A. The email included the three invention disclosures as an attachment, which is provided in Exhibit B.

5. In the ordinary course of business and in due time, a substantially finalized draft of the patent application was prepared by Kevin Barner, formerly of SUGHRUE MION, PLLC. I reviewed the draft of the patent application and provided my comments to Mr. Barner by email attachment on October 10, 2001. A copy of the email is attached as Exhibit C. A copy of the marked-up draft patent application is attached as Exhibit D.

6. The draft patent application provided in Exhibit D fully supports at least the independent claims of the filed patent application. Thus, it is clearly demonstrated that I conceived of the invention as recited in each of the independent claims of the filed patent application no later than October 10, 2001.

7. In the time between October 10, 2001 and the filing of the patent application on January 29, 2002, due diligence was exercised in constructively reducing the invention to practice. Modifications to the draft patent application were transmitted between Mr. Barner and me on several occasions by email during that time. Those emails are attached as Exhibit E.

8. In the ordinary course of business and in due time, the patent application was finalized. The patent application was then filed on January 29, 2002.

DECLARATION UNDER 37 CFR §1.131
U.S. APPLICATION NO. 10/424,922

9. In view of the foregoing, it is clear that I, the named inventor of the above-captioned application, invented the subject matter of the claims prior to the October 25, 2001 filing date of U.S. Provisional Application No. 60/330,608. In particular, Exhibits C and D demonstrate that I conceived of the invention no later than October 10, 2001. Further, the evidence shows that due diligence was exercised on constructively reducing the invention to practice from a time prior to October 21, 2001 to the constructive reduction to practice date (i.e., U.S. filing date) of January 29, 2002.

I hereby declare further that all statements made herein are of my own knowledge and are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Date: 23/10/06

Jonathan Goldstone

Unknown

From: Mandir, William H.
Sent: Tuesday, October 17, 2006 10:14 AM
To: Leman, Michael E.
Subject: FW: New file -Inventor: Jonathan Goldstone our file #75

goldstone - 3IDRs-.zip (15 KB)...

```
-----Original Message-----
From: Kvatinsky, Hananel [mailto:Hananel_Kvatinsky@icomverse.com]
Sent: Monday, March 05, 2001 6:20 AM
To: William H. Mandir (E-mail)
Cc: Goldstone, Jonathan
Subject: New file -Inventor: Jonathan Goldstone our file #75
```

Shalom Bill

I attach a compressed word file with 3 seperate disclosures by Jonathan Goldstone (same invetor as in Q60463).
As all disclosures are closely related, it is our will to incorporate into one application. Please let me know if this is possible.

Please prepare and file a US patent application. As usual, send me an estimated time schedule and cost.

regards

Hananel
<<goldstone - 3IDRs-.zip>>

Hananel Kvatinsky
Intellectual Property Manager

<<...OLE_Obj...>>

Comverse
29, Habarzel St. Tel Aviv 69710, Israel

Tel: +972-3-766-9374
Cellular: +972-58-54-9374
Fax : +972-3-645-2855, 766-9374
E-mail: hananel.kvatinsky@comverse.com

□

USSN 10/058,189

EXHIBIT A

General Information

Name of Inventor	1) Jonathan Goldstone	2)
Israeli Identity Number (ת.ז.)	309864411	
Work Location	Tel Aviv	
Work Number	972-3-6452482	
Work E-mail	Jonathan_goldstone@icomverse.com	
Start Date at Comverse	June 5 1994	
Home & mailing address	Tchernakovsky 6/6, Jerusalem 92581. Israel	
Country of Citizenship	UK, Israel	
Manager's Name	Doron Segal	

1) If there are more than one inventors, what did each inventor contribute to the invention?

Inventor 1: ______________________________

Inventor 2: ______________________________

Inventor 3: ______________________________

2) Are there inventors who do not work at Comverse today? If so:

One) Who are they?

Two) Where do they work now?

Three) Did they at work at Comverse at any time during the conception or implementation of the invention?

Four) If so, what are the dates that they started and stopped working at Comverse?

II. History of the Invention: *[The idea here is to let the lawyers know how the idea developed and at what stage of development the idea is today. The questions below should be answered very briefly.]*

1) What is the current stage of the idea? Select one: Concept __x___; Analysis ____; Design ___x___; Prototype ______; Bench Test/Alpha Test _______; Pilot Run/Beta Test __________; Commercial Production __________.

2) Conception of the idea:

One) When did the inventors get the idea for the invention (approximately, if the exact date is not known)? 11/00 – 1/01

Two) Where did this happen? CNS

Three) Where there any non-inventors present when the idea was created? No

Four) If so, who? No

USSN 10/058,189

EXHIBIT B

3) First sketch or drawing:
None made as yet.
One) When was the first sketch or drawing of the idea made?
Two) Who made it?
Three) If you have a copy of the first sketch or drawing, please attach it.

4) First model or prototype:
N/A
One) Was a model or prototype of the idea made?
Two) If so, when was the model or prototype completed?
Three) If this is being done now, when do you expect to complete the model or prototype?

5) Alpha testing:
N/A
a) Was the idea alpha tested?
One) Who performed the alpha test?
Two) When was the idea alpha tested?
Three) Apart from the inventors, who else was present during the alpha testing of the idea?
Four) Where was the idea alpha tested?

6) Beta testing (at a customer site or partner site):
N/A
a) Was the idea beta tested?
Five) Who performed the beta test?
Six) When was the idea beta tested?
Seven) Apart from the inventors, who else was present during the beta testing of the idea?
Eight) Where was the idea beta tested?

7) Has the idea been produced commercially? If so, when, how many units were produced (approximately), by who (that is, who was the manufacturer), and for who (that is, who was the customer)?
N/A
8) Does this invention impact the project you are working on? If so:
The areas of encrypted email upon UM systems was a problem that I faced in my previous task as IP Network & Security Group Manager, early in 2000. No adequate solution was found at that time. In the elapsed time I have considered the problem & tried to solve it. The results are shown in this draft application.

The concept of authenticated voicemail messaging has no basis in an actual project (apart from my general work in the security field) but would seem to be of vital importance to the main business of CNS.
One) How does the invention impact on your project?
Two) How would you categorize the amount of the impact on your project? VITAL [V] IMPORTANT [ ], or HELPFUL [ ]

(REMEMBER, A PATENT DOES NOT NEED TO BE AN INVENTION OF A TOTALLY NEW INDUSTRY. IT SIMPLY NEEDS TO BE SOMETHING NEW THAT HAS SOME TECHNICAL OR COMMERCIAL VALUE. SMALL OR MODERATE IMPROVEMENTS MAKE UP THE VAST MAJORITY OF ALL PATENTS, AND HIGHLY REGARDED BY COMVERSE.)

Three) Why did you pick that category for the impact on your project?

9) Apart from any impact the invention may have on your project, does this invention impact the Company's technology in general? If so:

Yes – all are directly applicable to one or several Comverse products.

One) How does the invention impact on your project?

Two) How would you categorize the amount of the impact on your project? VITAL [ ] IMPORTANT [ ], or HELPFUL [ ]

(AGAIN, THE GREAT MAJORITY OF PATENTS ARE SMALL OR MODERATE IMPROVEMENTS, WITH SOME TECHNICAL OR COMMERCIAL VALUE. ALL THESE PATENTS ARE RESPECTED AND REWARDED BY COMVERSE.)

c) Why did you pick that category for the impact on the Company's technology?

10) Prior Practice:

No

One) Was the invention practiced before in Comverse? If so, describe the circumstances?

Two) Was the invention practiced before at some place other than elsewhere? If so, describe the circumstances?

Three) Have you seen this solution in writing in the professional media?

Four) Have you performed a patent search? If so, did you find any patents that were relevant to the invention (even if they weren't exactly the same)? If so, what the numbers of those patents? (Attach copies of whatever relevant patents you have.) Even if you have not performed a patent search, have you seen this idea described in a different patent? - No

Five) Have you seen a similar idea described anywhere else? If so, under what circumstances? (That is, a competitor's product, an advertisement, a trade show, etc.) No

Six) Do you have regular access to trade magazines, technical articles? Do visit trade shows, or do you get trade show information from other people? - Yes

Seven) Where did you get the idea? – See 8 above.

C. Contacts with Outside Parties:

1) Up to the date you fill out this form, did you or anyone else you know of ever discuss the idea of the invention or the invention itself with anyone outside of Comverse? If so:

No

One) With whom outside of Comverse?

Two) When?
Three) Where?
Four) What were the circumstances? (Discussion of idea, or product demonstration, or market research, or testing, or joint development, or offer to sell, or sale, etc.)
Five) Were samples supplied?
Six) Were written drawings or diagrams supplied?
Seven) At the time of each such contact with an outside party, did Comverse have a Non-Disclosure Agreement between Comverse and the party? If so, do you have this Agreement or do you know who does have the Agreement? (If you have it, please attach a copy.)

2) Did you or anyone else at Comverse make an oral or written offer to sell? If so, please describe this offer, including name of potential customer, price offered, result of the offer, etc.

No

3) Do you or anyone you know of plan to discuss the idea of the invention or the invention itself with anyone outside of Comverse within the next six (6) months? If so, what will be the circumstances of this discussion? (Again, include any planned discussion, demonstration, market research, testing, joint development, offer to sell, intent to sell, etc.)

I understand that the encrypted email is a current problem. I have had no detailed discussion with the technical people involved.

4) Up to the date you fill out this form, was the idea ever published publicly? Does the idea appear in any Comverse promotional literature? Does the idea appear in any article or paper that was published? Was the idea ever presented at a trade show?

No

5) Up to the date you fill out this form, was there ever any other public announcement or other revelation of the idea of the invention or the invention itself? If so, when and under what circumstances? (An article, a trade show, a meeting, etc.)

No

6) Do you know if anyone is planning any public announcement or other public revelation of the idea of the invention or the invention itself over the next six (6) months? If so, when and under what circumstances?

No

Title: "A Method of Allowing an Email Provider or Operator to Play Shared Secret Encrypted Emails as Email to Speech etc services without Significantly Degrading Security"

Description

This patent describes a method to allow intermediate network equipment to access received shared secret encrypted emails or encrypted attachments without degrading the implied security. The purpose is to allow the recipient a choice of delivery method. For example, Email to Speech, Email to Fax, Email to SMSC, Email to WAP etc.

Prior Art

The technology of transforming a received email to a different format (Email To X) is well understood and it is not the intention of this patent to change existing methods. The advantages of these techniques are that they allow more immediate receipt of email contents. It allows the recipient to be "unplugged" from their laptop or PC and really get the message on the go. This is particularly relevant if the recipient is notified (phone call, SMS etc) that the email has been received.

Encrypting emails (or attachments within an email) is a necessary requirement in order to protect the content privacy. Some methods also have the advantage of ensuring that the email is sent by an authenticated source (not by an imposter) and that the contents are untampered upon receipt. The perceived need for such methods is clear, an email is stored and forwarded by a variety of devices between transmission and receipt and it is assumed that these devices are susceptible to tampering or eavesdropping by a variety of unknown parties. In many countries government agencies have the right to legally intercept messages.

When describing the transmission of a secure email it is conventional within the industry to use the example of Alice sending a message to Bob. This application will use the same convention.

This patent application focuses on a well-known method whereby Alice & Bob have a shared secret. This secret is effectively the cryptographic key to allow them to encrypt & decrypt messages. In this case the same key is used for both encryption & decryption of the message or attachment. The secret is established out of band to the actual transmission for example by phone, face to face at a previous meeting etc.

There are a variety of (free and commercial) packages available to do this. There are sites on the Internet that allow content encryption and Network Associates Inc offer a freeware and commercial package that allows an email attachment to be encrypted as a self decrypting archive (SDA). It is assumed that there are other similar packages available and that it is not impossible for a skilled artisan to replicate or enhance these offerings.

Most current handsets do not have the computational power to decrypt emails. Furthermore, there are some inherent advantages to receiving a spoken (eg when driving) or faxed version (eg a long complex mail) of the email. These features are best provided by the email service and not on the handset.

Problems with the Current Method

Currently, if an encrypted email is received then there is no reasonable method for the recipient to access it without being connected on line using their PC. It is accepted in the industry that a reasonable person receiving an encrypted email would not leave the decryption password stored on an operator's server where it could be legally or illegally intercepted. It is also reasonable to assume that the sender would prefer that the confidentially was not compromised in this way.

This essentially disables the Email To X transformations and requires a recipient to download the message and decrypt it locally on their own machine. This is the best solution in terms of security, but not very convenient if the recipient is on the move and cannot access the required information for several hours.

Solution

The proposed solution is that upon receipt of an encrypted email or attachment the recipient would be alerted in the normal way. The system would inform the recipient that the message was from the sender, the subject, but that the content was encrypted. The recipient would then have the choice to leave access for a later time when they could connect in the standard method and decrypt the message locally or to offer the system the password.

The password could be offered in a variety of methods:

- By DTMF – either an entirely numerical password, or by spelling out words in the way that is common with US phone numbers.
- By Voice Recognition – using voice recognition technology to recognize the password.
- By Mobile Originated Short Message – the recipient would send a short message to the system containing the password.

These methods could be further enhanced by using voice authentication methods to ensure that the recipient was indeed the recipient before accepting the password.

The assumptions behind this method are that this gives both the sender and the recipient control over which messages may be played using this technique. For example they may have two shared secrets, one for normal confidentiality and one for top secret. They may establish a shared secret just for this transaction etc.

In this way the message is delivered to the recipients email provider in a completely secure method. The fact that the password is revealed to the system is a low risk because as explained it is previously agreed by both parties that this is acceptable. The password could be stored by the system to decode another email conversation but that would require special design and could easily be defeated by changing passwords.

What is New?

The novelty in this application comprises the merging of the shared secret/SDA method with the Email To X. There is no current method that allows secure access to emails without the use of the recipients PC.

Title: "A Method of Allowing an Email Provider or Operator to Play Public Key Infrastructure (PKI) Encrypted Emails as Email to Speech etc services without Significantly Degrading Security"

Description

This patent describes a method to allow intermediate network equipment to access received PKI encrypted emails or encrypted attachments without degrading the implied security. The purpose is to allow the recipient a choice of delivery method. For example, Email to Speech, Email to Fax, Email to SMSC, Email to WAP etc.

Prior Art

The technology of transforming a received email to a different format (Email To X) is well understood and it is not the intention of this patent to change existing methods. The advantages of these techniques are that they allow more immediate receipt of email contents. It allows the recipient to be "unplugged" from their laptop or PC and really get the message on the go. This is particularly relevant if the recipient is notified (phone call, SMS etc) that the email has been received.

Encrypting emails (or attachments within an email) is a necessary requirement in order to protect the content privacy. Some methods also have the advantage of ensuring that the email is sent by an authenticated source (not by an imposter) and that the contents are untampered upon receipt. The perceived need for such methods is clear, an email is stored and forwarded by a variety of devices between transmission and receipt and it is assumed that these devices are susceptible to tampering or eavesdropping by a variety of unknown parties. In many countries government agencies have the right to legally intercept messages.

When describing the transmission of a secure email it is conventional within the industry to use the example of Alice sending a message to Bob. This application will use the same convention.

This patent application focuses on a well-known method known as Public Key Infrastructure.

In this technique an email subscriber applies to a recognized third party known as a Certificate Authority (CA). The CA may require proof that the applicant is who he/she claims to be (standard practice if the applicant is a corporation) or may accept the application at face value and offer a lower level of authentication as a result. The CA will generate a pair of keys known as the private key and the public key. These keys are mathematically related in that a message encrypted with one can only be decrypted using the other one. (Depending upon the key length) decrypting a message without the other key (for example, using a brute force try every combination attack, or by comparing previous messages etc) is considered to be sufficiently difficult as to be impossible.

The private key is transmitted to Bob and it his responsibility to ensure that the key does indeed remain private. Typically it is an alphanumeric string that is kept on his computer in a secure method.

If Alice wishes to send a message to Bob she needs to obtain Bob's public key. She does this either through a priori knowledge from a previous conversation, or by accessing the CA and asking for Bob's public key. Alice can now encrypt her message using Bob's public key. The message is now considered secure for the entire transmission, both interception on the wire or when stored by intermediate computers. The email can only be decrypted by Bob using his private key or by someone else that has gained access to his private key.

The whole system depends upon the reliability of the CA and the reliability & discretion of the certificate owner to keep the private key private.

The public private key system can also be used for authentication and integrity. If Alice signs her message with her private key before transmission then by using her public key Bob can verify that the message did come from Alice and not from an imposter. If the private key is used to guarantee a mathematical property of the message (the hash) then by using Alice's public key Bob can ensure that the message received is a true representation of the message that Alice sent.

These are extra reasons to ensure that the private key is kept private.

Most current handsets do not have the computational power to decrypt emails. Furthermore, there are some inherent advantages to receiving a spoken (eg when driving) or faxed version (eg a long complex mail) of the email. These features are best provided by the email service and not on the handset.

Problems with the Current Method

Currently, if an encrypted email is received then there is no reasonable method for the recipient to access it without being connected on line using their PC. As explained above the whole system relies upon the private keys being kept private. It is therefore accepted in the industry that a reasonable person receiving an encrypted email would not leave their private key stored on an operator's server where it could be legally or illegally intercepted. It is also reasonable to assume that the sender would prefer that the confidentially was not compromised in this way.

This essentially disables the Email To X transformations and requires a recipient to download the message and decrypt it locally on their own machine. This is the best solution in terms of security, but not very convenient if the recipient is on the move and cannot access the required information for several hours or longer.

Solution

The proposed solution is that the email operator with the Email to X capability (acting as the intended recipient's home mailbox) will provide a facility that may be regarded as "Bob Proxy." The Bob Proxy will have a private public key pair. In this case the private key would be kept in a secure fashion in a neutral area of the Bob Proxy identity. The private key would itself be encrypted with a password that was known only to Bob.

When first establishing Bob proxy, Bob would apply for a key pair in the normal fashion. He would then encrypt the private key using another password (a variety of techniques are possible) and transfer this to the system to act as Bob Proxy.

Alice wishing to send an email to Bob would have the choice of sending the email directly to Bob & thereby guaranteeing maximum security but preventing Bob from receiving the email in any Email to X method. Alternatively Alice could choose to send the email to Bob Proxy with a priori knowledge that this is a fairly secure alias for Bob that allows Bob to receive the emails in a variety of formats but that the private key is ultimately less secure than that of Bob himself.

Bob would be able to enhance the security of Bob Proxy by defining a series of rules; for example only certain senders would be accepted, messages of a certain length, with a certain subject, sent at certain time, from certain email hosts. This allows Bob a reasonable control a priori of messages that he is willing to accept in this fashion.

If the incoming email meets the restrictions imposed by Bob then the email will be accepted and Bob will be informed by the system that an encrypt email has been received by Bob Proxy. The message will inform Bob of the e-mail's characteristics. Bob could instruct the system to encrypt it further using his own public key or indeed to delete the message immediately.

Bob would then have the choice of logging on in the conventional manner or to instruct the system to process the message using one of the Email to X methods. The system would then have to request the password to decode the private key pair.

The password could be offered in a variety of methods:

- By DTMF – either an entirely numerical password, or by spelling out words in the way that is common with US phone numbers.
- By Voice Recognition – using voice recognition technology to recognize the password.
- By Mobile Originated Short Message – the recipient would send a short message to the system containing the password.

These methods could be further enhanced by using voice authentication methods to ensure that the recipient was indeed the recipient before accepting the password.

Upon receipt of the password the system would go to the neutral area and request the decrypted private key and then use this to decode the message to play it using the required Email to X method.

If the incoming email fails to meet Bob's criteria then a variety of options maybe set by Bob:

- The email is immediately rejected and a notice is sent by the System Administrator specifying that the email was sent to Bob Proxy and that the sender is requested to use Bob's personal public key to encode the message and to send it to Bob's secure email address.
- The email is encrypted using Bob's public key and stored in Bob's email or Bob Proxy's email inbox. This message can now only be decoded by Bob using his own private key.

The assumptions behind this method are that this gives both the sender and the recipient control over which messages may be played using this technique

Bob may restrict which messages can be accepted in the Bob proxy account. Equally a sender can choose to send or not to send a message to Bob Proxy.

In this way the message is delivered to the recipient's email provider in a completely secure method. The fact that the password is revealed to the system is a low risk because as explained it is further protected and ultimately is part of the working practice of the system. Trivially, Bob could change the key pair on a frequent basis and change the password required to access the private key on a very frequent basis.

A Further Enhancement

As a further enhancement a special Certificate Authority system could be established where the private key is stored by an independent third party that is unrelated to the email operator. This third party could even be located in a different legal jurisdiction. Upon receipt of an encrypted email to Bob Proxy, Bob could decide to accept or reject the email.

If Bob chooses to accept the email the decoded email (by using the private key) must be retrieved from the third party.

This could be achieved in several ways:

- Bob could provide the password used to decrypt the private key, (using any of the variety of methods listed above or other appropriate methods such as a series of identifying questions (answers known only to & predefined by Bob) or voice authentication.) This information would then be forwarded to the third party together with the encrypted email. The third party would decrypt the email using Bob Proxy's private key. The plain text message would then be encrypted using the email provider's public key and then sent back to the email provider. The email provider would then use its own private key to decrypt the message into a plain text message. This plain text message could then be used to perform the required Email to X functionality.
- The email provider would provide Bob with a unique identifier for the email & would forward the encrypted email to the third party. Bob would access his account at the third party identify himself (using any of the variety of methods listed above or other appropriate methods such as a series of identifying questions (answers known only to & predefined by Bob) or voice authentication). Bob would also supply the unique identifier relating to the email. The third party would decrypt the email using Bob Proxy's private key. The plain text message would then be encrypted using the email provider's public key and then sent back to the email provider. The email provider would then use its own private key to decrypt the message into a plain text message. This plain text message could then be used to perform the required Email to X functionality.

This enhancement whilst making the procedure more complex adds increased security. The private key is never known to the operator, and Bob has the choice of supplier of the private key deposit. This could be a third party or indeed a machine under Bob's control (such as his corporate server.)

In the event that there is a compromise then this would relate to a single message only. As previously explained there is a degree of control over even this risk due to the filtering on Bob proxy and the sender's choice to use Bob Proxy and not Bob.

Note that PKI has several options that affect the level of security (specifically key length); some of these are restricted by law in some jurisdictions. The methods presented here are independent of particular implementation. The implied security is primarily a function of the PKI implementation together with the modifications presented in this application.

What is New?

The novelty in this application comprises the merging of the Public Key Infrastructure method with the Email To X. This allows the benefits of the inherent security of PKI together with the mobility enhancements offered by the Email to X services. There is no current method that allows secure access to emails without the use of the recipient'ss PC.

Important Note
This patent application can be modified/rewritten in order to use similar ideas to facilitate secure mobile commerce (M-commerce).

Title: "An Enhanced Method of Allowing an Email Provider or Operator to Play Public Key Infrastructure (PKI) Encrypted Emails as Email to Speech etc services, by using one time passwords. The playing does not significantly degrading Security"

Description

This patent describes a method to allow intermediate network equipment to access received PKI encrypted emails or encrypted attachments without degrading the implied security. The purpose is to allow the recipient a choice of delivery method. For example, Email to Speech, Email to Fax, Email to SMSC, Email to WAP etc.

Prior Art

The technology of transforming a received email to a different format (Email To X) is well understood and it is not the intention of this patent to change existing methods. The advantages of these techniques are that they allow more immediate receipt of email contents. It allows the recipient to be "unplugged" from their laptop or PC and really get the message on the go. This is particularly relevant if the recipient is notified (phone call, SMS etc) that the email has been received.

Encrypting emails (or attachments within an email) is a necessary requirement in order to protect the content privacy. Some methods also have the advantage of ensuring that the email is sent by an authenticated source (not by an imposter) and that the contents are untampered upon receipt. The perceived need for such methods is clear, an email is stored and forwarded by a variety of devices between transmission and receipt and it is assumed that these devices are susceptible to tampering or eavesdropping by a variety of unknown parties. In many countries government agencies have the right to legally intercept messages.

When describing the transmission of a secure email it is conventional within the industry to use the example of Alice sending a message to Bob. This application will use the same convention.

This patent application focuses on a well-known method known as Public Key Infrastructure.

In this technique an email subscriber applies to a recognized third party known as a Certificate Authority (CA). The CA may require proof that the applicant is who he/she claims to be (standard practice if the applicant is a corporation) or may accept the application at face value and offer a lower level of authentication as a result. The CA will generate a pair of keys known as the private key and the public key. These keys are mathematically related in that a message encrypted with one can only be decrypted using the other one. (Depending upon the key length) decrypting a message without the other key (for example, using a brute force try every combination attack, or by comparing previous messages etc) is considered to be sufficiently difficult as to be impossible.

The private key is transmitted to Bob and it his responsibility to ensure that the key does indeed remain private. Typically it is an alphanumeric string that is kept on his computer in a secure method.

If Alice wishes to send a message to Bob she needs to obtain Bob's public key. She does this either through a priori knowledge from a previous conversation, or by accessing the CA and asking for Bob's public key. Alice can now encrypt her message using Bob's public key. The message is now considered secure for the entire transmission, both interception on the wire or when stored by intermediate computers. The email can only be decrypted by Bob using the private key or by someone else that has gained access to the private key.

The whole system depends upon the reliability of the CA and the reliability & discretion of the certificate owner (Bob) to keep the private key private.

The public private key system can also be used for authentication and integrity. If Alice signs her message with her private key before transmission then by using her public key Bob can verify that the message did come from Alice and not from an imposter. If the private key is used to guarantee a mathematical property of the message (the hash) then by using Alice's public key Bob can ensure that the message received is a true representation of message that Alice sent.

These are extra reasons to ensure that the private key is kept private.

Most current handsets do not have the computational power to decrypt emails. Furthermore, there are some inherent advantages to receiving a spoken (eg when driving) or faxed version (eg a long complex mail) of the email. These features are best provided by the email service and not on the handset.

Problems with the Current Method

Currently, if an encrypted email is received then there is no reasonable method for the recipient (Bob) to access it without being connected on line using their PC. As explained above the whole system relies upon the private keys being kept private. It is therefore accepted in the industry that a reasonable person receiving an encrypted email would not leave their private key stored on an operator's server where it could be legally or illegally intercepted. It is also reasonable to assume that the sender would prefer that the confidentially was not compromised in this way.

This essentially disables the Email To X transformations and requires a recipient (Bob) to download the message and decrypt it locally on their own machine. This is the best solution in terms of security, but not very convenient if the recipient is on the move and cannot access the required information for several hours or longer.

Solution

The proposed solution is that the email operator with the Email to X capability (acting as the intended recipient's home mailbox) will provide a facility that may be regarded as "Bob Proxy."

When first establishing Bob proxy, Bob would apply for a key pair in the normal fashion. He would then encrypt the private key using another password (a variety of techniques are possible) and transfer this to the system to act as Bob Proxy. This process could be repeated an arbitrary number of times to establish several key pairs. Each private key would be stored with a different access password. The private keys would be stored in a neutral area, each protected by an individual password.

When Alice attempts to look up Bob Proxy in order to obtain the certificate, then she will receive (randomly) one of the public keys with a short expiry time of several minutes, together with a notice explaining why the expiry time is so close. Once a public key is issued then this public-private key pair would be disabled and not issued again.

[This system could be modified slightly so that the key pairs were not generated in advance, but on demand when Alice attempts to look up Bob Proxy's certificate. In this case the single use private key would be stored on the system. So there is a trade off of easier use against lower protection of the private key.]

When the message is received then the time stamp would be checked to ensure that it originated in the short time window allowed by the certificate. If not then the message would be discarded.

If Alice wishes to send an email to Bob, she would have the choice of sending the email directly to Bob & thereby guaranteeing maximum security but preventing Bob from receiving the email in any Email to X method. Alternatively, Alice could choose to send the email to Bob Proxy with a priori knowledge that this is a fairly secure alias for Bob that allows Bob to receive the emails in a variety of formats but that the private key is ultimately less secure than that of Bob himself.

Bob would be able to enhance the security of Bob Proxy by defining a series of rules; for example only certain senders would be accepted, messages of a certain length, with a certain subject, sent at certain time, from certain email hosts, margin allowed on the time window. This allows Bob a reasonable control a priori of messages that he is willing to accept in this fashion.

If the incoming email meets the restrictions imposed by Bob then the email will be accepted and Bob will be informed by the system that an encrypt email has been received by Bob Proxy. The message will inform Bob of the e-mail's characteristics and which key pair is used (based on time or other means.) Bob could instruct the system to encrypt it further using his own public key or indeed to delete the message immediately.

Bob would then have the choice of logging on in the conventional manner or to instruct the system to process the message using one of the Email to X methods. The system would then have to request the password to decode the private key pair.

The password could be offered in a variety of methods:

- By DTMF – either an entirely numerical password, or by spelling out words in the way that is common with US phone numbers.
- By Voice Recognition – using voice recognition technology to recognize the password.
- By Mobile Originated Short Message – the recipient would send a short message to the system containing the password.

These methods could be further enhanced by using voice authentication methods to ensure that the recipient was indeed the recipient before accepting the password.

Upon receipt of the password the system would go to the neutral area and request the decrypted private key and then use this to decode the message to play it using the required Email to X method.

If the incoming email fails to meet Bob's criteria then a variety of options maybe set by Bob:

- The email is immediately rejected and a notice is sent by the System Administrator specifying that the email was sent to Bob Proxy and that Alice is requested to use Bob's personal public key to encode the message and to send it to Bob's secure email address.
- The email is encrypted using Bob's public key and stored in Bob's email or Bob Proxy's email inbox. This message can now only be decoded by Bob using his own private key.

The assumptions behind this method are that this gives both the sender and the recipient control over which messages may be played using this technique

Bob may restrict which messages can be accepted in the Bob proxy account. Equally, Alice can choose to send or not to send a message to Bob Proxy.

In this way the message is delivered to the recipient's email provider in a completely secure method. The fact that the password is revealed to the system is a low risk because it can only affect a single message. Trivially, Bob could change the key pair on a frequent basis and change the password required to access the private key on a very frequent basis.

A Further Enhancement

As a further enhancement a special Certificate Authority system could be established where the private keys are stored by an independent third party that is unrelated to the email operator. This third party could even be located in a different legal jurisdiction. Upon receipt of an encrypted email to Bob Proxy, Bob could decide to accept or reject the email.

If Bob chooses to accept the email the decoded email (by using the private key) must be retrieved from the third party.

This could be achieved in several ways:

- Bob could provide the password used to decrypt the private key. It could be supplemented by a series of identifying questions (answers known only to & predefined by Bob) or voice authentication. This information would then be forwarded to the third party together with the encrypted email. The third party would decrypt the email using Bob Proxy's private key. The plain text message would then be encrypted using the email provider's public key and then sent back to the email provider. The email provider would then use its own private key to decrypt the message into a plain text message. This plain text message could then be used to perform the required Email to X functionality.
- The email provider would provide Bob with a unique identifier for the email & would forward the encrypted email to the third party. Bob would access his account at the third party identify himself (using any of the variety of methods listed above or other appropriate methods such as a series of identifying questions (answers known only to & predefined by Bob) or voice authentication). Bob would also supply the unique identifier relating to the email. The third

party would decrypt the email using Bob Proxy's private key. The plain text message would then be encrypted using the email provider's public key and then sent back to the email provider. The email provider would then use its own private key to decrypt the message into a plain text message. This plain text message could then be used to perform the required Email to X functionality.

This enhancement whilst making the procedure more complex adds increased security. The private key is never known to the operator, and Bob has the choice of supplier of the private key deposit. This could be a third party or indeed a machine under Bob's control (such as his corporate CA.) Furthermore, the fact that each message is encrypted with a unique key pair makes the security very high.

In the event that there is a compromise then this would relate to a single message only. As previously explained there is a degree of control over even this risk due to the filtering on Bob proxy and the sender's choice to use Bob Proxy and not Bob.

Note that PKI has several options that affect the level of security (specifically key length); some of these are restricted by law in some jurisdictions. The methods presented here are independent of particular implementation. The implied security is primarily a function of the PKI implementation together with the modifications presented in this application.

What is New?

The novelty in this application comprises the merging of the Public Key Infrastructure method with the Email To X. This allows the benefits of the inherent security of PKI together with the mobility enhancements offered by the Email to X services. There is no current method that allows secure access to emails without the use of the recipient's PC.

Furthermore the use of a one-time key pair implementation significantly increases the security and reduces the risk of a compromise.

Important Note
This patent application can be modified/rewritten in order to use similar ideas to facilitate secure mobile commerce (M-commerce).

Unknown

From: Goldstone, Jonathan [Jonathan.Goldstone@comverse.com]
Sent: Wednesday, October 10, 2001 1:40 AM
To: kbarner@sughrue.com
Cc: Kvatinsky Hananel
Subject: ENCRYPTED E-MAIL RETRIEVAL SYSTEM
Importance: High

Hi Kevin

Firstly best wishes to you and your family. It is certainly trying times all over, but my sympathy & best wishes to those of you who are in the eye of the storm.

Many thanks for the recent draft. I have reviewed the document & enclose my comments as revision marks. In general there are a few typos, a couple of omissions that I didn't spot in previous reviews.

There is one substantial point - should the enhancement that relates to locating the proxy independently of the email provider actually be an independent embodiment. The case for the defence is that this is a central enhancement/feature to the basic ideas. I am happy to be guided by you on this issue as I think that the real basis for decision is the correct legal style of a patent application.

I am sorry that we are not quite there yet. In any case I hope that we are very close.

Regards,

Jonathan

USSN 10/058,189

EXHIBIT C

ENCRYPTED E-MAIL RETRIEVAL SYSTEM

FIELD OF THE INVENTION

The present invention relates generally to a communication system that allows for the retrieval of encrypted messages through different mediums media?. In particular, in accordance with one embodiment of the invention, encrypted attachments to a an e-mail message, transmitted over a communication network using one medium, such as a computer transmitting over a wide area network accessing the Internet, are recognized and decrypted by the intended e-mail recipient using a second, different, network medium, such as a cellular phone, pager, personal digital assistant (PDA), etc. By utilizing either symmetric or asymmetric encryption technology, the integrity of the encrypted e-mail message, and its attachment, is maintained.

BACKGROUND OF THE INVENTION

The technology of transforming a received e-mail to a different format, i.e., e-mail-to-voice or e-mail-to-facsimile data, etc., is well known in the art. One advantage gained by employing these techniques is that format transformation of the e-mail message oftentimes permits the intended recipient of the message to receive the message more quickly than if such transformations were unavailable. For example, an e-mail user may physically be at a location which is inconvenient for receiving e-mail messages, such as in his or her car or in a meeting. In order to guarantee immediate receipt of e-mail messages, the user may have his e-mail messages forwarded from his computer, which is physically connected to the e-mail network, to his cellular phone, pager, PDA, fax machine or any other device that will make retrieval of the e-mail more convenient.

Accordingly, when an e-mail message is received by the recipient's computer, the message is converted into an appropriate format and transferred to the recipient's cellular phone, etc. Upon receipt of the message, the phone then indicates receipt of the message, i.e., by activating an audible and/or visual alarm recognized by the recipient. The recipient can then identify the respective sender of the message and/or subject and determine whether or

USSN 10/058,189

EXHIBIT D

not to retrieve the message immediately, defer receipt until a later time, or delete the message without opening it.

One issue that concerns virtually all e-mail users is the security of the content of the messages sent. Because e-mail messages are typically sent over the Internet, from one network to another, they are subject to being passed through various devices between the time the message leaves the sender's machine until it reaches the recipient's machine. Each one of the various devices the e-mail message, and any corresponding attachments, passes through along its journey is capable of copying and/or altering the message content, thus, exposing the message content to mailcious interceptions. Also, in some countries, government agencies routinely monitor e-mail message content. Accordingly, it has become a favorable practice among e-mail users to encrypt private or otherwise sensitive material that either party, sender or recipient, desires to remain confidential.

Encryption, or cryptography, is the technique of converting plain information into unintelligible information and re-converting the unintelligible information back into an intelligible, preferably the original, form. Cryptography has existed for centuries but it has recently been given significantly more attention as a result of the advent of e-commerce, privacy concerns and the Internet. Faster, cheaper, higher-powered computers and communications systems are enabling the development of new cryptographic systems and methodologies and, along with them, the ability to crack/decipher the codes.

One conventional encryption technique is referred to as the "shared secret" technique. The shared secret technique consists of a single mathematical "key" used for both encryption and decryption of data. This type of cryptographic system is sometimes also referred to as "symmetric" cryptography because the same "key" both encrypts and decrypts the message. Both the sender and the recipient of a message, such as an e-mail message, must possess the same mathematical key and the parties are responsible for physically maintaining the secrecy and security of the key to ensure the privacy and security of their communication.

In shared secret, or symmetrical, encryption, the sender of a message encrypts the message using any of a virtually limitless number of encryption algorithms. Upon receipt of the message on the recipient's computer, after being passed through various intermediary machines as an encrypted message, the recipient decrypts the message by using the same algorithm, in reverse, as the sender used to encrypt the message. Obviously, in order for this system to work, the sender and the recipient must each know which algorithm was used to send the message. Accordingly, the parties typically agree on an algorithm through various "offline" means, such as a private telephone conversation, a separate e-mail, etc.

Another encryption technique, one that improves upon the "shared secret" method, is known as "Public Key" cryptography. Public Key cryptography employs a two-key system wherein the two keys are asymmetric, or completely different. However, even though the two keys are different, they comprise a set and work together to encode and decode information. One key is kept private, or secret, by one of the parties and the other key is made readily available to the public, however, it is typically retained in a trustworthy repository. When a public key is used to encrypt a message, only the private key from the pair is capable of decrypting the message. Thus, in public key cryptography, anyone can send secret messages to the holder of a private key because the matching public key is readily available, yet no one other than the intended recipient, who possesses the matching private key, can decrypt the message. Therefore, regardless of the number of people that come into possession of the message, the integrity of the message content is maintained.

Public Key cryptography has lead to several other useful innovations, such as the digital signature. A digital signature is much like a hand-written signature in that it provides proof that the originator of the message is actually who the person claims to be (a process known as "Authentication"). A sender "signs" messages by passing them through a mathematical algorithm, known as a "hash" function, and produces a summary, or "hash", of the subject message. Mathematically, this summary, or hash, is unique for every message, similar to the way a fingerprint is unique for every person. The sender then encrypts the hash with his private key and attaches the code to the end of the message. This attached code is the digital signature. The intended recipient, upon receipt of the encrypted message and sender signature, verifies the authenticity of the message and proves that it has not been

Deleted: T

altered in transit by decrypting the digital signature with the sender's public key and passing the message through the same hash function, in reverse. If the two hash codes are the same, it can be confirmed that the message was indeed sent from the holder of the matching private key (Non-repudiation) and that it was not altered (Integrity).

A Public Key Infrastructure (PKI) refers to the entire Public Key system. A PKI comprises the keys as well as one or more trusted systems known as Certification Authorities (CA). These CAs are organized in a tree-like hierarchical structure. Each user's Public Key and identification are placed in a digital certificate. The CA digitally signs each certificate and makes the certificates freely available by publishing them in publicly accessible directories. Any client, or user, of the PKI may access any other user's Public Key and verify the authenticity by using the CA's Public Key to verify the CA's signature on the certificate. The CA at the top of the hierarchy signs certificates of subordinate CAs and these CAs in turn sign certificates of CAs below themselves and so forth. This system establishes a chain of trust in a distributed CA system., including cryptographic keys and a certificate management system. The PKI enables secure transactions and private exchange of information between parties who may either be well known to each other or complete strangers. PKI provides privacy, integrity, authentication, and non-repudiation for applications and electronic commerce transactions.

There are a variety of free and commercial packages available for performing either type of encryption, i.e., symmetrical and/or asymmetrical. There are also websites on the Internet that allow content encryption and companies that offer software packages for encryption. Network Associates, Inc., for example, offers a freeware and a commercial package that allow an e-mail attachment to be encrypted as a self decrypting archive (SDA). It is assumed that there are other similar packages available and that it is possible for a skilled artisan to replicate or enhance these offerings.

However, most current handsets, e.g., wireless phones, pagers, PDAs, etc., do not have the computational power to decrypt e-mails that are coded using these methods. A key can be considered secure if it can not be cracked in a reasonable time by brute force (i.e., trying all combinations sequentially), even if cracking the key requires using many computers. The security of a key, i.e., its ability to withstand attempts to decipher it, is in relation to its length. In other words, the longer the actual mathematical code used to create the key, the more difficult it becomes to decode/decipher it and, thus, the more secure it is. However, decoding long keys makes the job of the handset more difficult. In the handset, low computational power prefers short simple and, therefore, insecure codes.

Currently, when an encrypted e-mail is received, there is no reasonable method for the recipient to access it without being connected on-line using his PC. It is accepted in the industry that a reasonable person receiving an encrypted e-mail would not leave the decryption password stored on an operator's server where it could be legally, or illegally, intercepted. It is also reasonable to assume that the sender would prefer that confidentiality not be compromised in this way.

Accordingly, in accordance with conventional methods, a recipient of an encrypted e-mail, in order to maintain the integrity of the message, is required to download the message and decrypt it locally on his own secure machine. The recipient, even if notified of the receipt of an e-mail message, on his phone, PDA, pager, etc., will not be able to view it, or listen to it immediately without compromising the messages integrity, i.e., without providing the decryption "key" on the open system. In most cases this also compromises future messages that will typically use the same password. This becomes, as a minimum, an inconvenience to the recipient, and possibly to the sender, when the recipient is mobile and not physically located where secure message retrieval is possible.

SUMMARY OF THE INVENTION

In view of the aforementioned problems with the conventional approach to e-mail encryption and delivery, it is an object of the present invention to provide a communication system in which encrypted e-mail messages and/or their corresponding attachments, can be decrypted and converted to another format to be delivered to some other device other than the recipients main, secure, machine (PC). A further object of the present invention is to perform the above-mentioned message conversion and delivery without significantly compromising the integrity of the message content.

In accordance with one embodiment of the present invention, a system is provided in which an e-mail recipient is notified of; (1) receipt of an e-mail message; (2) the sender's identity; (3) the subject of the message; and (4) an indication of whether the message is encrypted. The recipient then has the choice of either downloading the message on a secure machine at a later time or opening the message immediately by providing the system with the appropriate decryption key. According to this embodiment, the shared secret/SDA method and the e-mail-to-other format techniques are joined. Currently, there is no known method that allows secure access to coded e-mails in the absence of a significant amount of computational power while simultaneously offering the recipient a convenient method of message retrieval while the recipient is mobile.

In accordance with another embodiment of the present invention, a system is provided in which an e-mail recipient is notified, either by his normal e-mail provider or by a previously arranged proxy server, of receipt of an e-mail message; the sender's identity; a subject of the message; and an indication of whether the message is encrypted. The recipient then has the choice of either downloading the message on a secure machine at a later time, further encrypting the message using his own public key, deleting the message or having the system process the message using one or more of any available e-mail-to-other format techniques.

In accordance with yet another embodiment of the present invention, a system is provided in which an e-mail recipient is notified, either by his normal e-mail provider or by a previously arranged proxy server, of receipt of an e-mail message; the sender's identity; a subject of the message; and an indication of whether the message is encrypted. The recipient then has the choice of either downloading the message on a secure machine at a later time or opening the message immediately by using the one respective private key corresponding to one of a variety of public keys used to encrypt the message.

BRIEF DESCRIPTION OF THE DRAWINGS

The object and features of the present invention will become more readily apparent from the following detailed description of the preferred embodiments taken in conjunction with the accompanying drawings in which:

FIG. 1 is a diagrammatic view of a first embodiment of the present invention.

FIG. 2 is a diagrammatic view of a second embodiment of the present invention.

FIG. 3 is a diagrammatic view of a third embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiments of the present invention are discussed in detail below. While specific configurations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without departing from the spirit and scope of the invention.

Embodiment 1

In accordance with a first embodiment of the present invention, in reference to Figure 1, the sender 10 of an encrypted e-mail message, sends the message, along with any corresponding attachment(s), through the Internet 20, or some other similar network, to the intended recipient's e-mail server 30. Upon receipt of the encrypted e-mail message by the recipient's e-mail server 30, the recipient 40 is alerted by activation of an audible and/or visual notification 45. Further, within the message 47, the e-mail server 30 informs the recipient 40 of; (1) the sender's identity, (2) the subject of the message and (3) whether the content of the message is encrypted. Small style point – 45 should be before 47 (ie higher)? Also we should show 57 the transfer of the decrypted email.

Recipient 40 then has the choice of deferring message retrieval for a later time, when the recipient can conveniently connect in the standard method, e.g., using a secure machine 50 connected to his e-mail server 30, where he can decrypt the message locally, or retrieving the message immediately by offering the e-mail server 30 the password, or shared secret 55. As illustrated by the thick dashed line, connecting the recipient 40 to the recipient's secure machine 50, if the recipient decides to defer message retrieval until a later time, he will need to travel to the location of the secure machine 50, and cannot retrieve the message remotely, as is possible using the latter option.

The password, or shared secret 55, can be offered using a variety of different methods. For example;

- By Dual Tone Multi-Frequency (DTMF) – either an entirely numerical password, or by spelling out words on an alphanumeric keypad;
- By Voice Recognition – using voice recognition technology to recognize the password; or,
- By Mobile Originated Short Message – the recipient would send a short message to the system containing the password.

The present embodiment can be further enhanced by using a voice authentication method to ensure that the person attempting retrieval of the message is indeed the intended recipient 40. For obvious reasons, a voice authentication method is preferably performed in the e-mail server 30, which is likely a dedicated server that is part of the total system, prior to accepting the password, or shared secret 55. Also known question mechanism. An advantage associated with the above-mentioned technique is that it gives both the sender 10 and the recipient 40 control over which messages are retrieved, and when they are retrieved. To provide further flexibility and an additional degree of security, the parties may have two, or more, shared secrets, one for normal confidentiality and one for highly confidential, or "top secret" material. Additionally, the parties can establish a shared secret for a single particular transaction. Those skilled in the art would be able to derive other various techniques for transferring the password 55 to the e-mail server 30 without venturing from the spirit of the present invention.

According to the present embodiment, an encrypted e-mail message is delivered to the recipient's e-mail server in a completely secure method since it is encrypted. Then, the recipient is immediately notified of receipt of the message, i.e., through conventional cellular, or other, communication methods, and the recipient has the option of providing the server with the decryption key, or password, in order to have the decrypted message converted into a proper format and transmitted to the recipient. The fact that the password is revealed to the server carries a much lower risk than would otherwise be born since the password is only shared with the server, directly from the recipient, and does not pass through various other machines where it is susceptible to being intercepted. Also, as explained above, it is agreed by both parties, prior to the sender sending the message, that this level of risk is acceptable. Although the likelihood is remote, it is possible that the password would be intercepted by an unscrupulous third party, "listening" in on the recipient's mobile communication channel, and used to attempt to decode additional e-mail messages directed to the recipient. However, this type of risk can be easily obviated by the parties agreeing to change passwords either after each transmission or at least often enough to minimize the risk of having a third party obtain and use the password.

Although the present embodiment has been described using cellular technologies, this embodiment, as well as other embodiments, is not limited to the intended message recipient receiving the message via cellular technologies. For example, the message recipient could receive the messages on a public computer where Internet browsing is enabled.

Deleted: u

Embodiment 2

In accordance with a second embodiment of the present invention, in reference to Figure 2, the e-mail server 30 with e-mail-to-other format capability (acting as the intended recipient's home mailbox) provides a facility known as the recipient's "Proxy" 60. Proxy 60 should have some connection to the Internet The Proxy 60 maintains a private/public key pair to be used in the event the recipient 40 receives an encrypted e-mail message and can be located virtually anywhere. For example, proxy 60 can be located at the recipient's e-mail server 30 or it can be located in an entirely different location. The private key is kept in a secure fashion in a neutral area of the Proxy 60 identity and, if desired, can itself be encrypted with a password known only by the recipient 40.

Deleted: a

When first establishing the Proxy 60, the recipient 40 applies for a key pair. Subsequently, after the key pair has been established, the recipient 40 encrypts the private key with yet another password using any of a variety of different known techniques, and transfers the encrypted private key to the system to act as his Proxy 60. The sender 10, wishing to send an e-mail to the recipient 40 chooses whether to have the server 30 send the e-mail directly to the recipient's secure machine 50 (using a dedicated key pair & email address), thereby guaranteeing maximum security but preventing the recipient 40 from receiving the e-mail in any e-mail-to-other format method, or sending the e-mail to the Proxy 60 with *a priori* knowledge that the Proxy 60 is a fairly reasonably? secure alias for the recipient.

As mentioned previously, in connection with the first embodiment, as represented by the thick dashed line in Figure 2, connecting recipient 40 and secure machine 50, if the recipient decides to defer message retrieval until a later time, when he can retrieve and decrypt the message in a more secure manner on secure machine 50, he must physically go to the location of secure machine 50. The sender 10 would typically be aware that sending the encrypted e-mail message to the Proxy 60 allows the recipient 40 to receive the e-mail in a variety of formats but that sending the e-mail to the Proxy 60 and using the private key to decrypt its contents is ultimately slightly less secure than sending the e-mail message directly to the recipient's secure machine 50. Of course, the use of a proxy, as described with respect to this embodiment, is not limited to a private/public key scheme. Other encryption/decryption methods, such as the shared secret scheme discussed above, may also be used with the proxy.

The recipient 40 can enhance the security of the Proxy 60 by defining a series of rules limiting the e-mail traffic allowed to enter the Proxy 60. For example, rules could be derived in the Proxy where only e-mail messages from certain specified senders would be accepted. Further, messages of a specified length, with a specified subject, sent during a specified time and/or sent from certain e-mail hosts, can be either deleted upon receipt or transferred directly to the recipient's secure system, i.e., the system where decryption can be carried out without the need for transmitting the password or key information over another network or through another, third party, machine. Accordingly, the recipient is afforded reasonable control over messages that he is willing to accept in this fashion.

If the incoming e-mail meets the restrictions imposed by the recipient's rules, the e-mail will be accepted by the Proxy and the recipient will be informed by the system that an encrypted e-mail has been received by the Proxy. The recipient will also be informed of certain characteristics corresponding to the e-mail message, such as sender's identity, subject, length, whether there is any attachments, etc. The recipient then instructs the Proxy 60 to encrypt the message further, using his own public key or, possibly, instructs the Proxy to delete the message.

In accordance with the present embodiment, after determining whether to retrieve the e-mail message, the recipient 40 then decides whether to retrieve the message via his own secure system 50, or whether to instruct the Proxy 60 to decrypt and process the message using one of the e-mail-to-other format methods. If the recipient 40 decides to have the Proxy 60 send him the decrypted e-mail, the Proxy then requests the necessary password 55 from the recipient 40 to decode the private key. If the password is accepted by the proxy 60 the message is decrypted 65 and delivered to the recipient 40 in the specified format.

As mentioned in regard to the previous embodiment, the password can be offered using a variety of methods:

- By Dual Tone Multi-Frequency (DTMF) – either an entirely numerical password, or by spelling out words on an alphanumeric keypad;
- By Voice Recognition – using voice recognition technology to recognize the password; or,
- By Mobile Originated Short Message – the recipient would send a short message to the system containing the password.

These methods could be further enhanced by using voice authentication methods to ensure that the party acting on behalf of the recipient indeed has the authority to do so. For example, voice codes could be stored within the Proxy 60 and prior to accepting any password 55 from a party attempting to act on behalf of the recipient 40, the party's voice could be checked against the stored voice codes to verify authorization. Other, seemingly simpler methods, may also be employed, such as a challenge request where a user is asked to answer a question to which only the user knows the answer, i.e., the maiden name user's mother. This also applies to all other descriptions.

Upon receipt of the authorized password 55, the Proxy 60 accesses its neutral area and requests the decrypted private key and uses the decrypted key to retrieve the encrypted e-mail message. Using the required e-mail-to-other format method to convert the message to the format required by the recipient at that time, i.e., voice for a receiving the message over a cellular phone, facsimile data for receiving the e-mail over facsimile machine, etc., the Proxy 60 then delivers the formatted, decrypted message 65 to the recipient 40.

On the other hand, if the incoming e-mail fails to meet the recipient's criteria, established in the Proxy 60, a variety of options can be employed by the recipient 40. For example, the e-mail can be immediately rejected and a notice sent by the System Administrator of server 30 indicating that the e-mail was sent to the Proxy 60 and, further, requesting that the sender 10 use the recipient's personal public key to encode the message and send it to the recipient's secure e-mail address on secure machine 50. Alternatively, in the Proxy 60, the e-mail message and/or its attachment(s) can be encrypted if it has not yet been encrypted, or it can be further encrypted if it has already been encrypted by the sender 10. Because this particular encryption is performed within the Proxy 60, the recipient's public key, which was stored in the Proxy when the Proxy was initialized, as discussed previously, can be used. The encrypted, or further encrypted, e-mail message is then stored in the recipient's secure e-mail inbox 50 or in the recipient's Proxy e-mail inbox 60. The encrypted e-mail message can now only be decoded by the recipient using his own private key.

An advantage associated with the present, second, embodiment is that, similar to the first embodiment described above, it provides both the sender 10 and the recipient 40 control over which messages are retrieved, how they are received, and when. Additionally, further protection is provided for e-mail messages retrieved using a system in accordance with the second embodiment since the recipient 40 can restrict which messages are accepted in the Proxy account. Also, a sender can choose to send or not send a message to the Proxy.

Also the password is never transmitted over the air, it is not disclosed at the point of requirement but is set up in advance - possibly months earlier.

In accordance with this embodiment, the message is delivered to the recipient's e-mail provider 30 in a manner that is completely secure. This mechanism could be further enhanced with a password selection mechanism that offers single-use, randomly distributed, passwords, discussed later. The fact that the password is revealed to the system carries minimum risk because, as explained previously, it is further protected and ultimately is part of the working practice of the system. Furthermore, the recipient could frequently change the key pair and he could also change the password required to access the private key even more frequently. Accordingly, it would be virtually impossible to intercept and decode encrypted e-mail messages unless the interceptor had the precise key at the precise time and he also was able to gain authorization for supplying the key by getting around the voice recognition, password, or other such authorization system employed.

According to a further enhancement to this embodiment, a special Certificate Authority system is established where the private key is stored by an independent third party that is unrelated to the e-mail operator 30. This third party could even be located in a different legal jurisdiction. Upon receipt of an encrypted e-mail by the recipient's Proxy 60, the recipient 40 can then decide to accept or reject the e-mail. If the recipient chooses to accept the e-mail, the decrypted e-mail, decrypted using the private key, is retrieved from the third party. I wonder if this should not be a separate embodiment with its own diagram – what do you think? Reason being that this is a main idea in the patent & could really be an enhancement to all the other embodiments. Alternatively I accept the current treatment of showing it as an enhancement to both embodiments 2 & 3 – it is your call as a strict legal question.

This retrieval can be achieved in several ways. For example, the recipient 40 could provide the password used to decrypt the private key, using any of the variety of methods listed above, as well as any other appropriate method. Other appropriate methods include techniques such as querying a series of identifying questions where the predefined answers are known only to the recipient, as discussed above, or voice authentication. Results of these security checks are then forwarded to the third party together with the encrypted e-mail. The third party would decrypt the e-mail using the Proxy's private key. The plain text message would then be encrypted using the e-mail provider's public key and then sent back to the e-mail provider. The e-mail provider would then use its own private key to decrypt the message into a plain text message. This plain text message could then be used to perform the required e-mail-to-other format conversion.

The e-mail provider 30 can provide the recipient 40 with a unique identifier for the e-mail and would also forward the encrypted e-mail to the third party. The recipient 40 could access his account at the third party himself, using any of the variety of methods listed above or other appropriate methods such as a series of identifying questions, etc.

The encrypted email is supplied to the third party together with an identifier. Upon authorization (described below) the third party decodes the email and passes it back to the email server.

The recipient 40 also supplies the unique identifier relating to the e-mail. The third party decrypts the e-mail using the recipient's Proxy private key. This decrypted email should be protected. Protection methods include using the email servers public private key (as described below), using a dedicated, secure communications channel, using a VPN (virtual private network) to establish a secure channel in an otherwise public Internet, or by any other appropriate methods.

The plain text message is then encrypted using the e-mail provider's public key and the message is sent back to the e-mail provider. The e-mail provider then uses its own private key to decrypt the message into a plain text message. This plain text message could then be used to perform the required e-mail-to-other format conversion as desired.

It is important to note that the private key or shared password is never made available to the email server. Also the methods described elsewhere to increase security by changing passwords are equally applicable here.

In accordance with this enhancement to the present embodiment of the invention, even though the additional procedures make the overall procedure more complex, they add increased security to the system. The private key is never known to the operator, and the recipient has the choice of supplier of the private key. The supplier of the private key can be a well-trusted third party or it can even be a separate machine that is under the control of the recipient, such as his corporate email server.

In the event an encrypted message is compromised, i.e., for some reason a third party was able to intercept the recipient's key pair and decrypt the encrypted e-mail message, the degree to which the system is compromised is limited to that one particular message. This is really only true in the option for single-use pairs. As previously described, there is a degree of control over even this risk due to the filtering on the Proxy 60 and the sender's choice to use the Proxy 60 and not the recipient's secure machine 50. Also, time expiration methods are inherent within the certificate schemes. It is assumed that the proxy methods described here will include frequent changes of passwords possibly even to one time usage.

A system operating under a PKI has several options that affect the level of security (specifically key length); some of these are restricted by law in some jurisdictions. The methods in accordance with the embodiments of the present invention are independent of any single particular implementation. The afforded security is primarily a function of the PKI implementation together with the unique adaptations provided by the present invention.

The present embodiment comprises merging Public Key Infrastructure (PKI) techniques with e-mail-to-other format methods. This merger allows the benefits of the inherent security of PKI together with the mobility enhancements offered by the e-mail-to-other format services. Again, presently, there exists no method that allows secure access to e-mails without the direct use of the recipient's PC, or some other dedicated machine with sufficient processing power. As mentioned above in regard to embodiment 1, the invention is not limited to cellular technologies, other mechanisms, such as public Internet browsers, etc., can be used to access messages.

Embodiment 3

In accordance with a third embodiment of the present invention, referring to Figure 3, an e-mail server 30 with e-mail-to-other format capability, and acting as the intended recipient's home mailbox, similar to the second embodiment, also provides a facility that may be regarded as the recipient's "Proxy" 60.

When first establishing the Proxy 60, the recipient 40 typically applies for a key pair in the normal fashion, as discussed previously. The recipient 40 then encrypts the private key using another password (as already discussed, a variety of techniques are possible) and transfers the encrypted key to the facility acting as the recipient's Proxy 60. In accordance with this embodiment, the process of establishing a key pair and encrypting the private key is repeated an arbitrary number of times to establish several secure key pairs. Each private key can be stored with a different access password in a neutral area of the Proxy 60.

When a sender 10 attempts to look up the recipient's Proxy 60 in order to obtain the certificate, the sender 10 randomly receives one of the public keys with a short expiration time, i.e., several minutes, together with a notice explaining the short expiration time. Once a public key is issued to the sender 10, that particular public-private key pair is disabled and not issued again.

As an enhancement, a system in accordance with this embodiment can be modified slightly so that the key pairs are not generated in advance, but rather on demand when the sender 10 attempts to look-up the recipient's Proxy's certificate. In this situation, the single-use private key would be stored on the system. Accordingly, there is a trade-off between ease of use and a reduction in the protection afforded by the private key.

When the e-mail message is ultimately received, a time stamp that is typically included in the message overhead is checked to ensure that the message was originated in the short time window allowed by the certificate. If the time stamp indicates that the message originated outside the allotted time, the message is discarded. If the sender 10 wishes to send an e-mail to the recipient 40, she would have the choice of sending the e-mail directly to the recipient's secure machine 50, thereby guaranteeing maximum security but preventing the recipient from receiving the e-mail in any e-mail-to-other format. Alternatively, the sender 10 can choose to send the e-mail to the recipient's Proxy 60 with *a priori* knowledge that this is a fairly secure alias for the recipient which allows the recipient 40 to receive e-mails in a variety of formats.

Similar to the second embodiment, discussed above, the recipient can enhance the security of the Proxy 60 by defining a series of rules; for example only certain senders would be accepted, messages of a certain length, with a certain subject, sent at certain time, from certain e-mail hosts, margin allowed on the time window, etc. This allows the recipient reasonable control over messages that he is willing to accept in this fashion.

If the incoming e-mail meets the restrictions imposed by the recipient, the e-mail will be accepted and the recipient will be informed by the system that an encrypted e-mail has been received by the Proxy 60. The message will inform the recipient of the e-mail's characteristics and which key pair is used (based on time or other means). The recipient then instructs the Proxy 60 to encrypt the message further, using his own public key or, possibly, instructs the Proxy to delete the message.

In accordance with the present embodiment, after determining whether to retrieve the e-mail message, the recipient 40 then decides whether to retrieve the message via his own secure system 50, or whether to instruct the Proxy 60 to decrypt and process the message using one of the e-mail-to-other format methods. If the recipient 40 decides to have the Proxy 60 send him the decrypted e-mail, the Proxy then requests the necessary password 55 from the recipient 40 to decode the private key. If the password is accepted by the proxy 60 the message is decrypted 65 and delivered to the recipient 40 in the specified format.

As mentioned in regard to the previous embodiment, the password can be offered using a variety of methods:

- By Dual Tone Multi-Frequency (DTMF) – either an entirely numerical password, or by spelling out words on an alphanumeric keypad;
- By Voice Recognition – using voice recognition technology to recognize the password; or,
- By Mobile Originated Short Message – the recipient would send a short message to the system containing the password.

These methods could be further enhanced by using voice authentication methods to ensure that the party acting on behalf of the recipient indeed has the authority to do so. For example, voice codes could be stored within the Proxy 60 and prior to accepting any password 55 from a party attempting to act on behalf of the recipient 40, the party's voice could be checked against the stored voice codes to verify authorization. Also the known question mechanism.

Upon receipt of the authorized password 55, the Proxy 60 accesses its neutral area and requests the decrypted private key and uses the decrypted key to retrieve the encrypted e-mail message. Using the required e-mail-to-other format method to convert the message to the format required by the recipient at that time, i.e., voice for a receiving the message over a cellular phone, facsimile data for receiving the e-mail over facsimile machine, etc., the Proxy 60 then delivers the formatted, decrypted message 65 to the recipient 40.

On the other hand, if the incoming e-mail fails to meet the recipient's criteria, established in the Proxy 60, a variety of options can be employed by the recipient 40. For example, the e-mail can be immediately rejected and a notice sent by the System Administrator of server 30 indicating that the e-mail was sent to the Proxy 60 and, further, requesting that the sender 10 use the recipient's personal public key to encode the message and send it to the recipient's secure e-mail address on secure machine 50. Alternatively, in the Proxy 60, the e-mail message and/or its attachment(s) can be encrypted if it has not yet been encrypted, or it can be further encrypted if it has already been encrypted by the sender 10. Because this particular encryption is performed within the Proxy 60, the recipient's public key, which was stored in the Proxy when the Proxy was initialized, as discussed previously, can be used. The encrypted, or further encrypted, e-mail message is then stored in the recipient's secure e-mail inbox 50 or in the recipient's Proxy e-mail inbox 60. The encrypted e-mail message can now only be decoded by the recipient using his own private key, as distinguished from the slightly less secure proxy, private key.

An advantage associated with the present, third, embodiment is that, similar to the first embodiment described above, it provides both the sender 10 and the recipient 40 control over which messages are retrieved, how they are received, and when. Additionally, further protection is provided for e-mail messages retrieved using a system in accordance with the second embodiment since the recipient 40 can restrict which messages are accepted in the Proxy account. Also, a sender can choose to send or not send a message to the Proxy. The real advantage here that is different to the other embodiments is that there are many single use time restricted key pairs.

In accordance with this embodiment, the message is delivered to the recipient's e-mail provider 30 in a manner that is completely secure. The fact that the password is revealed to the system carries minimum risk because, as explained, it is further protected and ultimately is part of the working practice of the system. Furthermore, the recipient could frequently change the key pair and he could also change the password required to access the private key even more frequently. Accordingly, it would be virtually impossible to intercept and decode encrypted e-mail messages unless the interceptor had the precise key at the precise time and he also was able to gain authorization for supplying the key by getting around the voice recognition, password, or other such authorization system employed.

According to a further enhancement to this embodiment, a special Certificate Authority system is established where the private key is stored by an independent third party that is unrelated to the e-mail operator 30. This third party could even be located in a different legal jurisdiction. Upon receipt of an encrypted e-mail by the recipient's Proxy 60, the recipient 40 can then decide to accept or reject the e-mail. If the recipient chooses to accept the e-mail, the decrypted e-mail, decrypted using the private key, is retrieved from the third party.

This retrieval can be achieved in several ways. For example, the recipient 40 could provide the password used to decrypt the private key, using any of the variety of methods listed above, as well as any other appropriate method. Other appropriate methods include techniques, such as, querying a series of identifying questions where the predefined answers are known only to the recipient, or voice authentication. Results of these security checks are then forwarded to the third party together with the encrypted e-mail. The third party would decrypt the e-mail using the Proxy's private key. The plain text message would then be encrypted using the e-mail provider's public key and then sent back to the e-mail provider. The e-mail provider would then use its own private key to decrypt the message into a plain text message. This plain text message could then be used to perform the required e-mail-to-other format conversion.

The e-mail provider 30 can provide the recipient 40 with a unique identifier for the e-mail and would also forward the encrypted e-mail to the third party. The recipient 40 could access his account at the third party himself, using any of the variety of methods listed above or other appropriate methods such as a series of identifying questions, etc. From here to para start line 18 I prefer the wording in embodiment 2. The recipient 40 could also supply the unique identifier relating to the e-mail. The third party would decrypt the e-mail using the recipient's Proxy private key. The plain text message would then be encrypted using the e-mail provider's public key and the message would then be sent back to the e-mail provider. The e-mail provider then uses its own private key to decrypt the message into a plain text message. This plain text message could then be used to perform the required e-mail-to-other format conversion.

In accordance with this enhancement to the present embodiment of the invention, even though the additional procedures make the overall procedure more complex, they add increased security to the system. The private key is never known to the operator, and the recipient has the choice of supplier of the private key. The supplier of the private key can be a well-trusted third party or it can even be a separate machine that is under the control of the recipient, such as his corporate server.

In the event an encrypted message is compromised, i.e., for some reason a third party was able to intercept the recipient's key pair and decrypt the encrypted e-mail message, the degree to which the system is compromised is limited to that one particular message. As previously described, there is a degree of control over even this risk due to the filtering on the Proxy 60 and the sender's choice to use the Proxy 60 and not the recipient's secure machine 50.

A system operating under a PKI has several options that affect the level of security (specifically key length); some of these are restricted by law in some jurisdictions. The methods in accordance with the embodiments of the present invention are independent of particular implementation. The afforded security is primarily a function of the PKI implementation together with the unique adaptations provided by the present invention.

The third embodiment, similar to the second embodiment described above, comprises merging Public Key Infrastructure (PKI) techniques with e-mail-to-other format methods. This merger allows the benefits of the inherent security of PKI together with the mobility enhancements offered by the e-mail-to-other format services. However, in accordance with the third embodiment, the Proxy 60 is established with a predefined number of private-public key pairs, each protected by a respective password or access code. In this manner, the recipient can use each key pair once, thereby increasing the security of the system even further.

Also, in accordance with a further embodiment of the invention, when a public/private key pair is established, the public key is obtained by the sender through standard methods, as described previously, however, the private key is held by a Certificate Authority (CA) who maintains the security of the private key. The CA issues short-term "licenses" to use the private key, to specified users, upon receipt of an authorization grant provided by the recipient. The authorization grant is provided to the CA via a phone call or any other appropriate method as described previously. Further, the specified users of the short-term licenses include the recipient's own machine and/or the recipient's proxy. As mentioned above in regard to embodiment 1, the invention is not limited to cellular technologies, other mechanisms, such as public Internet browsers, etc., can be used to access messages.

A further enhancement that applies equally to all embodiments of the present invention involves having the sender specify in the transmitted message whether or not the message can be converted into another format, other than the format of the transmitted message, i.e., e-mail-to-other conversion. Also, the sender can be given the capability to generate a password, either randomly or by user input, and send the password to the intended recipient of the message. It is favorable to send the password to the recipient in an "out-of-band" method, such as by separate electronic message or by a forced phone message. Out-of-Band techniques are employed to provide security against outside persons, or machines, intercepting both the encrypted message and the password that can be used to invoke decryption.

WHAT IS CLAIMED IS:

1. An electronic message retrieval system comprising:

a sender operable to encrypt and transmit an electronic message, directed to a specified recipient, over a transmission medium;

a message retrieval device operable to receive the encrypted electronic message and provide an alarm message to a secondary device indicating that the encrypted electronic message has been received by the message retrieval device, wherein said secondary device is operable to receive messages in a format different from a format of the encrypted electronic message.

2. An electronic message retrieval system as claimed in claim 1, further comprising:

a secure device operable to receive and decrypt the encrypted electronic message from said message retrieval device, wherein said secure device is further operable to receive messages in the same format as the format of the encrypted electronic message.

3. An electronic message retrieval system as claimed in claim 1, wherein said message retrieval device comprises:

a converter device operable to convert the encrypted electronic message into a format recognized by the secondary device; and

a decryption device operable to decrypt the encrypted electronic message upon receipt of a password,

an output unit from which a decrypted and converted version of the encrypted electronic message is provided to the secondary device.

4. An electronic message retrieval system as claimed in claim 3, wherein said sender encrypts the electronic message in accordance with a specified electronic key and said message retrieval device decrypts the encrypted electronic message using said specified electronic key.

5. An electronic message retrieval system as claimed in claim 1, further comprising:

a password transmission unit operable to transmit a password to said specified recipient.

6. An electronic message retrieval system as claimed in claim 5, further comprising:

a password transmission path through which said password is transmitted to said recipient; and

a message transmission path, different from said password transmission path, through which said decrypted electronic message is provided to the recipient.

7. An electronic message retrieval system as claimed in claim 6, wherein said password is generated by the sender and communicated to the password transmission unit in a message different from the encrypted electronic message.

8. An electronic message retrieval system as claimed in claim 1, wherein said transmission medium is the Internet.

9. An electronic message retrieval system as claimed in claim 1, wherein said encrypted electronic message comprises an indication as to whether the encrypted electronic message can be converted into a different format.

10. An electronic message retrieval system comprising:

a sender operable to encrypt and transmit an electronic message directed to a specified recipient;

a message retrieval device operable to receive the encrypted electronic message and provide an alarm message to a secondary device when the encrypted electronic message is received by the message retrieval device, wherein said secondary device is operable to receive messages in a format different from the format of the encrypted electronic message, said message retrieval device comprising;

a converter device operable to convert the encrypted electronic message into a format recognized by the secondary device; and

a decryption device operable to decrypt the encrypted electronic message upon receipt of a password;

said electronic message retrieval system further comprising;

a secure device operable to receive and decrypt the encrypted electronic message, wherein said secure device is operable to receive messages in the same format as the format of the encrypted electronic message.

11. An electronic message retrieval method comprising:

sending an encrypted electronic message over a communication network to a recipient's message retrieving device;

alerting, with an alarm, a recipient of the receipt of the encrypted electronic message;

determining, based on summary information included in the alarm, whether to defer opening of the encrypted electronic message, or whether to open the encrypted electronic message immediately.

12. An electronic message retrieval method as claimed in claim 2, wherein;

if it is determined that opening the encrypted electronic message is to be deferred, receiving and decrypting said encrypted electronic message on a secure machine; and

if it is determined that opening the encrypted electronic message is to be performed immediately, providing a password to the recipient's message retrieving device to render the recipient's message retrieving device operable to decrypt the encrypted electronic message, and converting the encrypted electronic message into a format compatible with a secondary device from a format which is incompatible with the secondary device.

13. An electronic message retrieval method as claimed in claim 2, further comprising:

indicating to said recipient whether the encrypted electronic message can be converted into a format compatible with a secondary device from a format which is incompatible with the secondary device.

14. An electronic message retrieval method comprising:

sending an encrypted electronic message over a communication network to a recipient's message retrieving device;

alerting, with an alarm, a recipient of the receipt of the encrypted electronic message;

determining, based on summary information included in the alarm, whether to defer retrieval of the encrypted electronic message or retrieve the encrypted electronic message immediately; and if it is determined that retrieval of the encrypted electronic message is to be deferred, receiving and decrypting said encrypted electronic message on a secure machine; or

if it is determined that retrieval of the encrypted electronic message is to be performed immediately, providing a password to the recipient's message retrieving device to render the recipient's message retrieving device operable to decrypt the encrypted electronic message, and converting the encrypted electronic message into a format compatible with a secondary device from a format which is incompatible with the secondary device.

15. An electronic message retrieval system comprising:

a sender operable to encrypt and transmit an electronic message over a communication network directed to a specified recipient;

a message retrieval device operable to receive the encrypted electronic message and provide an alarm message to a secondary device when the encrypted electronic message is received by the message retrieval device;

a proxy device operable to receive the encrypted electronic message from the message retrieval device when the recipient provides a proxy instruction to said message retrieval device and operable to decrypt and transmit a decrypted electronic message to said recipient when the recipient provides a password to said proxy device.

16. An electronic message retrieval system as claimed in claim 3, further comprising:

a secure device operable to receive and decrypt the encrypted electronic message, wherein said secure device is operable to receive messages in the same format as the format of the encrypted electronic message.

17. An electronic message retrieval system as claimed in claim 3, wherein said encryption is performed by the sender using a publicly accessible key associated with the recipient.

18. An electronic message retrieval system as claimed in claim 3, wherein said proxy decrypts said encrypted electronic message by using a private key securely stored on said proxy.

19. An electronic message retrieval system as claimed in claim 3, wherein said secondary device is operable to receive messages in a format different from the format of the encrypted electronic message.

20. An electronic message retrieval system as claimed in claim 3, said proxy device comprising:

a converter device operable to convert the encrypted electronic message into a format recognized by the secondary device; and

a decryption device operable to decrypt an encrypted private key associated with the recipient and also decrypt the encrypted electronic message, wherein the decryption device is activated upon receipt of a password.

21. An electronic message retrieval system comprising:

a sender operable to encrypt and transmit an electronic message over a communication network directed to a specified recipient, wherein said encryption is performed using a publicly accessible key associated with the recipient;

a message retrieval device operable to receive the encrypted electronic message and provide an alarm message to a secondary device when the encrypted electronic message is received by the message retrieval device, wherein said secondary device is operable to receive messages in a format different from the format of the encrypted electronic message;

a proxy device operable to receive the encrypted electronic message from the message retrieval device when the recipient provides a proxy instruction, said proxy device comprising;

a converter device operable to convert the encrypted electronic message into a format recognized by the secondary device; and

a decryption device operable to decrypt an encrypted private key associated with the recipient and also decrypt the encrypted electronic message, wherein the decryption device is activated upon receipt of a password;

said electronic message retrieval system further comprising;

a secure device operable to receive and decrypt the encrypted electronic message, wherein said secure device is operable to receive messages in the same format as the format of the encrypted electronic message.

22. An electronic message retrieval method comprising:

sending an encrypted electronic message over a communication network to a recipient's message retrieving device, wherein said encryption is performed using a publicly accessible key associated with the recipient;

alerting the recipient, with an alarm, of the receipt of the encrypted electronic message;

determining, based on summary information included in the alarm, whether to defer retrieval of the encrypted electronic message or retrieve the encrypted electronic message immediately; and

if it is determined that retrieval of the encrypted electronic message is to be deferred, receiving and decrypting said encrypted electronic message on a secure machine; or if it is determined that retrieval of the encrypted electronic message is to be performed immediately, providing a password to a proxy device;

decrypting, in said proxy device, a private encrypted key associated with the recipient to render the proxy operable to decrypt the encrypted electronic message; and

converting the encrypted electronic message into a format compatible with a secondary device from a format which is incompatible with the secondary device.

23. An electronic message retrieval system comprising:

a sender operable to encrypt and transmit an electronic message over a communication network directed to a specified recipient, wherein said encryption is performed using one of a plurality of publicly accessible keys associated with the recipient;

a message retrieval device operable to receive the encrypted electronic message and provide an alarm message to a secondary device when the encrypted electronic message is received by the message retrieval device, wherein said secondary device is operable to receive messages in a format different from the format of the encrypted electronic message;

a proxy device operable to receive the encrypted electronic message from the message retrieval device when the recipient provides a proxy instruction, said proxy device comprising;

a converter device operable to convert the encrypted electronic message into a format recognized by the secondary device; and

a decryption device operable to decrypt a plurality of encrypted private keys associated with the recipient and also decrypt the encrypted electronic message, wherein the decryption device is activated upon receipt of one of a plurality of passwords respectively associated with said encrypted private keys;

said electronic message retrieval system further comprising;

a secure device operable to receive and decrypt the encrypted electronic message, wherein said secure device is operable to receive messages in the same format as the format of the encrypted electronic message.

24. An electronic message retrieval method comprising:

sending an encrypted electronic message over a communication network to a recipient's message retrieving device, wherein said encryption is performed using one of a plurality of publicly accessible keys associated with the recipient;

alerting the recipient, with an alarm, of thc receipt of the encrypted electronic message;

determining, based on summary information included in the alarm, whether to defer retrieval of the encrypted electronic message or retrieve the encrypted electronic message immediately; and

if it is determined that retrieval of the encrypted electronic message is to be deferred, receiving and decrypting said encrypted electronic message on a secure machine; or

if it is determined that retrieval of the encrypted electronic message is to be performed immediately, providing one of a plurality of passwords to a proxy device, said provided password being associated with the publicly accessible key used to encrypt the message;

decrypting, in said proxy device and upon receipt of said password, a private encrypted key associated with the publicly accessible key used to encrypt the message to render the proxy operable to decrypt the encrypted electronic message; and

converting the encrypted electronic message into a format compatible with a secondary device from a format which is incompatible with the secondary device.

25. An electronic message retrieval system comprising:

a sender operable to encrypt and transmit an electronic message, directed to a specified recipient, over a transmission medium;

a message retrieval device operable to receive the encrypted electronic message and provide an alarm message to a secondary device indicating that the encrypted electronic message has been received by the message retrieval device;

a message retrieval device operable to receive an alternate version of said encrypted electronic message, wherein said alternate version of said encrypted message is in a format different from a format of the encrypted electronic message.

ABSTRACT OF THE DISCLOSURE

An electronic message retrieval system in which the electronic message, and any corresponding attachments, can be encrypted by the sender of the message and routed to the intended recipient, even if the intended recipient is in a mobile location or it is otherwise inconvenient for the recipient to receive the electronic message in the form in which it was sent. The system provides an alarm or indication to the intended recipient, wherever he or she is, that a message has been delivered, an indication of the subject of the message and who sent the message, and whether the message is encrypted. The intended recipient then has the choice of deferring retrieval of the message until a later time when he or she can log onto a secure system and decrypt the message conventionally, or providing the system with a password or "key" which will permit the system to decrypt the message, convert it into a format retrievable by the mobile recipient, i.e., audible format for phone delivery, facsimile data for fax delivery, etc., and deliver the message to the mobile recipient.

PI

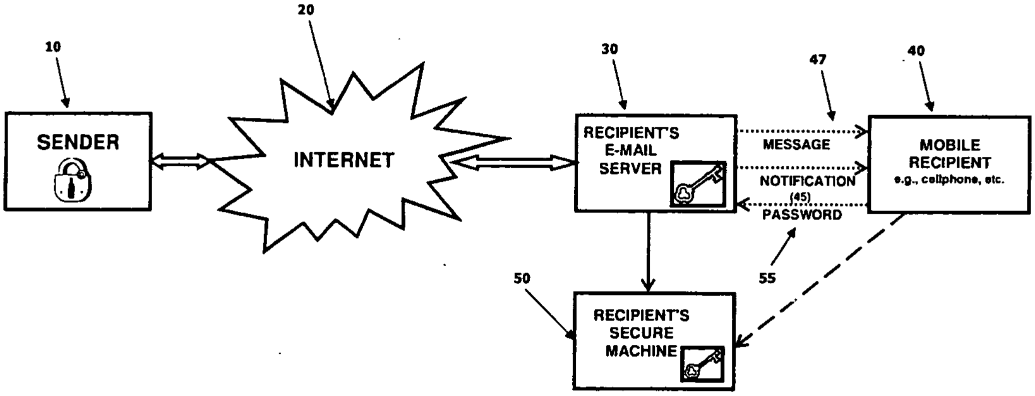
10
20
30
47
40
SENDER
INTERNET
RECIPIENT'S
E-MAIL
SERVER
MESSAGE
NOTIFICATION
(45)
PASSWORD
MOBILE
RECIPIENT
e.g., cellphone, etc.
50
55
RECIPIENT'S
SECURE
MACHINE

FIG. 1

PI

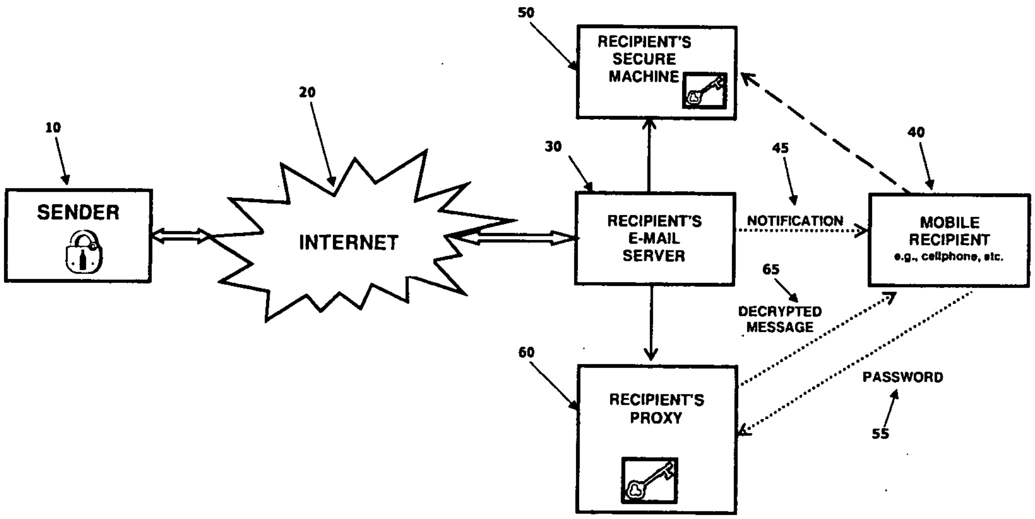
50
RECIPIENT'S SECURE MACHINE
20
10
30
45
40
SENDER
INTERNET
RECIPIENT'S E-MAIL SERVER
NOTIFICATION
MOBILE RECIPIENT
e.g., cellphone, etc.
65
DECRYPTED MESSAGE
60
RECIPIENT'S PROXY
PASSWORD
55

FIG. 2

Pf

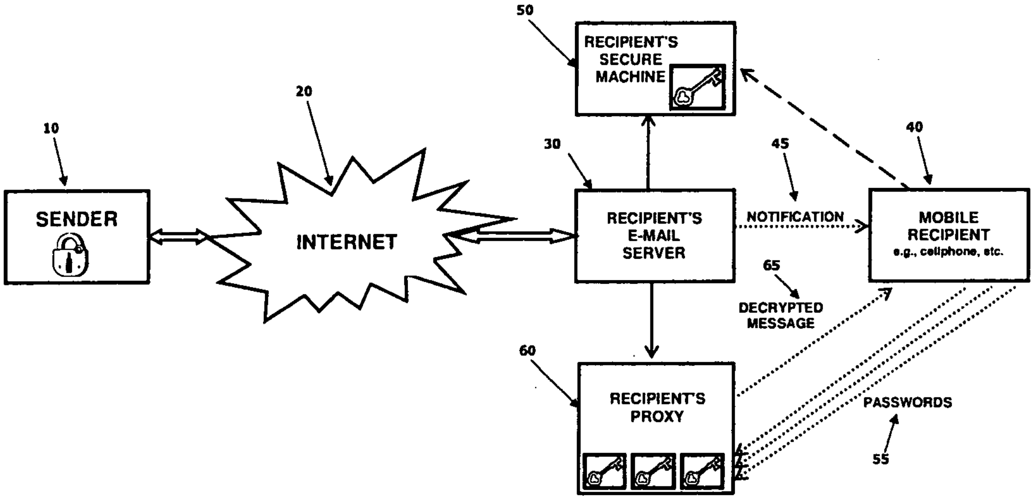
50
RECIPIENT'S SECURE MACHINE
20
10
30
45
40
SENDER
INTERNET
RECIPIENT'S E-MAIL SERVER
NOTIFICATION
MOBILE RECIPIENT
e.g., cellphone, etc.
65
DECRYPTED MESSAGE
60
RECIPIENT'S PROXY
PASSWORDS
55

FIG. 3

Barner, Kevin

From: Goldstone, Jonathan [jonathan_goldstone@icomverse.com]
Sent: Monday, December 31, 2001 12:05 AM
To: 'Barner, Kevin'
Cc: 'Mandir, William H.'; Kvatinsky, Hananel
Subject: RE: ENCRYPTED E-MAIL RETRIEVAL SYSTEM SUGHRUE REF Q63477 COMVERSE REF 703/US

Importance: High

Hi Kevin,

Many thanks for your prompt turn around. I trust that you had an enjoyable holiday season. I would like to wish you & all your nearest & dearest the very best for the new year. We all hope that it proves to be a better one.

Now to the matter in hand. Once again I wish to complement you on a superb job.

In general I like application and think that it is ready.

I have an annoying habit - every time somebody asks me to read a document (no matter how many times I have done already) I can always find something. So with that apology/caveat ....

1. I think that embodiment 5 is still a bit lightweight. Here is my suggestion. The "extras" are borrowed from embodiment 4. Please double check the reference numbers between the 2 diagrams.

[070] Referring to Figure 5, according to a fifth embodiment, a special Certificate Authority system is established in a system similar to the system of embodiment 3 where the private key is stored by an independent third party 70 that is unrelated to the e-mail operator 30. This third party, like the one described in embodiment 3, can be located in a different legal jurisdiction.

>>In accordance with this embodiment, the process of establishing a key pair and encrypting the private key is repeated an arbitrary number of times to establish several secure key pairs. Each private key can be stored with a different access password in a neutral area of the Proxy 60. password in a neutral area of the Proxy 60.
[058] When a sender 10 attempts to look up the recipient's Proxy 60 in order to obtain the certificate, the sender 10 randomly receives one of the public keys with a short expiration time, i.e., several minutes, together with a notice explaining the short expiration time. Once a public key is issued to the sender 10, that particular public-private key pair is disabled and not issued again.
[059] As an enhancement, a system in accordance with this embodiment can be modified slightly so that the key pairs are not generated in advance, but rather on demand when the sender 10 attempts to look-up the recipient's Proxy's certificate. In this situation, the single-use private key would be stored on the system. Accordingly, there is a trade-off between ease of use and a reduction in the protection afforded by the private key.
[060] When the e-mail message is ultimately received, a time stamp that is typically included in the message overhead is checked to ensure that the message was originated in the short time window allowed by the certificate. If the time stamp indicates that the message originated outside the allotted time, the message is discarded. If the sender 10 wishes to send an e-mail to the recipient 40, she would have the choice of sending the e-mail directly to the recipient's secure machine 50, thereby guaranteeing maximum

EXHIBIT E

security but preventing the recipient from receiving the e-mail in any e-mail-to-other format. Alternatively, the sender 10 can choose to send the e-mail 57 to the recipient's Proxy 60 with a priori knowledge that this is a fairly secure alias for the recipient which allows the recipient 40 to receive e-mails in a variety of formats. <<

Upon receipt of an encrypted e-mail 57 by the recipient's Proxy 60, the recipient 40 can then decide to accept or reject the e-mail. If the recipient chooses to accept the e-mail, the decrypted e-mail, decrypted using the private key, is retrieved from the third party 70.

✓2. Para 69 - I think that this is out of context for this embodiment. The possibility to change the key par is implicit in this embodiment. You may wish to borrow from para 78 which has a similar context.

3. We changed para 7 in the last correspondence. I missed one more point that needed correcting:

Obviously, in order for this system to work, the sender and the recipient must each know which Obviously, in order for this system to work, the sender and the recipient must each know which
>> (no - algorithm insert..) key<<
was used to send the message.

4. It is implicit in the entire application that the proxy or handling takes place at the email server or close by & under the control of the email provider. This is indeed the natural place. However, someone skilled in the art could do a similar thing based as a client application on each email recipients machine. We should probably protect against this with a comment in the "...skilled in the arts..." paragraph about the server is described for clarity but it is recognised that similar features can be provided on the client by someone skilled in the arts.

I hope that wasn't too bad..!!

As I am out of (email) touch after Mon 31/12 for 2 weeks I am more than happy for you to make the changes that you see fit & submit without further reference to me. If there are questions of substance then please just call me +972-54-322482 & I will do my best (I will take a copy of the document & this email with me.)

Now I have to start thinking about my 2002 patent!

Regards,

Jonathan

-----Original Message-----
From: Barner, Kevin [mailto:kbarner@sughrue.com]
Sent: Thursday, December 20, 2001 6:23 PM
To: Goldstone, Jonathan
Cc: Mandir, William H.; Kvatinsky, Hananel
Subject: RE: ENCRYPTED E-MAIL RETRIEVAL SYSTEM SUGHRUE REF Q63477 COMVERSE REF 703/US

Hi Jonathan,

Thank you for you latest comments. I have finalized the application in consideration of your comments and ask that you take one final look at the app.

Please pay particular attention to embodiment 5 (for which you offered comment no. 6 in your e-mail of Dec. 18.

Thanks for all your help with this application. I await your final approval.

Hananel - we will await your final approval before filing.

Best wishes for the new year.

Kevin

<<q63477 Draft App(F).doc>>

> -----Original Message-----
> From: Kvatinsky, Hananel [SMTP:Hananel_Kvatinsky@icomverse.com]
> Sent: Wednesday, December 19, 2001 12:51 AM
> To: Kevin Barner (E-mail)
> Cc: William H. Mandir (E-mail)
> Subject: FW: ENCRYPTED E-MAIL RETRIEVAL SYSTEM SUGHRUE REF Q63477
> COMVERSE REF 703/US
> Importance: High
>
> Hi Kevin
>
> I would appreciate if you could finalize the changes this week.
>
> This way I may be able to put it on George Jakobsche's desk before he goes
> to his Christmas - New Year Vacation
>
>
>
> Hananel
>
>
>
> Hananel Kvatinsky
> Intellectual Property Manager
>
>
>
>
> Comverse
> 29, Habarzel St. Tel Aviv 69710, Israel
>
> Tel: +972-3-766-9374
> Cellular: +972-58-54-9374
> Fax : +972-3-767-8486, 766-9374
> E-mail: hananel.kvatinsky@comverse.com
>
>
>
>
> -----Original Message-----
> From: Goldstone, Jonathan
> Sent: Tuesday, December 18, 2001 6:41 PM
> To: Barner, Kevin
> Cc: Kvatinsky, Hananel
> Subject: RE: ENCRYPTED E-MAIL RETRIEVAL SYSTEM
> Importance: High
>
>
> Hi Kevin,

>
> Many thanks.
>
> Here is my response:
>
> 1 Minor changes in para 7
> 2 I have added process ref numbers to embodiment 5
> 3 Para 78 question
> 4 Para 68
> 5 Para 70
> 6 I think that embod 5 relates to the multiple password CA case. I can not
> see an explicit reference to multiple passwords in the text. Note also
> that
> if so the many keys in fig 5 should be in the CA not in the proxy.
> 7 I did not check the what is claimed section.
>
> From my point of view you can make the changes based on my comments &
> file.
> If you wish me to review please use change marks as this will speed up my
> response.
>
> I assume that there is a strong motivation for us to file before end of
> January (end of financial year). I hope that the changes fall within this
> timeframe. Please note however that I am out of the office Jan 1-14 & I
> doubt that I will have access to email during this period. I am in Boston
> Tues - Thurs so if you have any questions please feel free to call me on
> +1-954-600-1321.
>
> Of course I would like to wish you & all yours Season's Greetings & a very
> Happy New Year.
>
> Regards
>
> Jonathan
>
>
>
> -----Original Message-----
> From: Barner, Kevin [mailto:kbarner@sughrue.com]
> Sent: Saturday, November 17, 2001 12:08 AM
> To: Goldstone, Jonathan
> Cc: Kvatinsky, Hananel; Mandir, William H.
> Subject: RE: ENCRYPTED E-MAIL RETRIEVAL SYSTEM
>
>
> Hi Jonathan,
>
> Attached is what I hope is a final draft. I have added two embodiments
> (now
> 3 and 5) which include the
> CA into embodiments 2 and 4 respectively. Also, I have added new figures
> 3
> and 5 which correspond to embs. 3 and 5 respectively.
> I added a few dependent claims as well to cover these embodiments.
>
> Please review the disclosure very closely for accuracy and
> comprehensiveness, paying particular attention to the new embodiments
> and their respective figures.
>
> I look forward to your comments.
>
> Best regards,
> Kevin
>

> <<q63477 Draft App(E).doc>>
>
> > -----Original Message-----
> > From: Goldstone, Jonathan [SMTP:jonathan_goldstone@icomverse.com]
> > Sent: Monday, October 29, 2001 8:13 AM
> > To: 'Barner, Kevin'
> > Cc: Kvatinsky, Hananel; Mandir, William H.
> > Subject:RE: ENCRYPTED E-MAIL RETRIEVAL SYSTEM
> >
> > Kevin
> >
> > How are you doing? Wishing you a very good week. I hope that things are
> > settling down over there to some type of tolerable normality, at least
> for
> > those not directly affected.
> >
> > I have answered the points that you raised and added a few more lines.
> My
> > comments are in revision marks as normal but in order to show the
> > distinction between my old comments & my new ones the new ones are
> > highlighted in yellow.
> >
> > Note that there is also a small item on fig 1
> >
> > I have produced a draft fig 4 covering the 3rd party CA. Note that
> >
> > 1. it is a separate document (Word problems)
> > 2. It needs a lot of editing to make it professional standard (apologies
> I
> > am graphically challenged & as we are not 100% sure that this is what we
> > want I restricted my cursing to the level of a draft!!)
> > 3. Depending on your decision on the legal why's of the draft we need to
> > produce a version of fig 3 showing the 3rd party CA & adapt some of the
> > text. Again I have left this until we agree on what line we want to
> take.
> >
> > Regards as always,
> >
> > Jonathan
> >
> >
> >
> > -----Original Message-----
> > From: Barner, Kevin [mailto:kbarner@sughrue.com]
> > Sent: Wednesday, October 24, 2001 9:55 PM
> > To: Goldstone, Jonathan
> > Cc: Kvatinsky, Hananel; Mandir, William H.
> > Subject: RE: ENCRYPTED E-MAIL RETRIEVAL SYSTEM
> >
> >
> > Jonathan,
> >
> > Thank you very much for your good wishes. Unfortunately, you too live
> in
> > a
> > part of the world where such things are all too familiar.
> >
> > Attached please find a revised version of the application. I have
> > substantially made the changes you suggested to both the spec and the
> > drawings.
> > However, I have a few questions regarding two of your
> > suggestions/questions.
> > They are embedded in the text next to your suggestions/questions.
> > I look forward to your response.

> >
> > Regards,
> > Kevin
> >
> > <<q63477 Draft App(C).doc>>
> >
> > > -----Original Message-----
> > > From: Goldstone, Jonathan [SMTP:jonathan_goldstone@icomverse.com]
> > > Sent: Wednesday, October 10, 2001 2:40 AM
> > > To: 'kbarner@sughrue.com'
> > > Cc: Kvatinsky, Hananel
> > > Subject: ENCRYPTED E-MAIL RETRIEVAL SYSTEM
> > > Importance: High
> > >
> > >
> > > Hi Kevin
> > >
> > > Firstly best wishes to you and your family. It is certainly trying
> times
> > > all
> > > over, but my sympathy & best wishes to those of you who are in the eye
> > of
> > > the storm.
> > >
> > >
> > > Many thanks for the recent draft. I have reviewed the document &
> enclose
> > > my
> > > comments as revision marks. In general there are a few typos, a couple
> > of
> > > omissions that I didn't spot in previous reviews.
> > >
> > > There is one substantial point - should the enhancement that relates
> to
> > > locating the proxy independently of the email provider actually be an
> > > independent embodiment. The case for the defence is that this is a
> > central
> > > enhancement/feature to the basic ideas. I am happy to be guided by you
> > on
> > > this issue as I think that the real basis for decision is the correct
> > > legal
> > > style of a patent application.
> > >
> > > I am sorry that we are not quite there yet. In any case I hope that we
> > are
> > > very close.
> > >
> > > Regards,
> > >
> > > Jonathan
> > > <<q63477 Draft App(B)withJSGcomments.doc>> << File: q63477 Draft
> > > App(B)withJSGcomments.doc >>
> > << File: q63477 Draft App(C)jsg-fig4.doc >> << File: q63477 Draft
> > App(C)jsg.doc >>